HELP WITH 9.2 AND 10.1

The following lemmata would be extremely useful for 9.2 and 10.1. There may be a way to tackle the problems without these insights, but I don't know how.

Notation (and conventions). p and q are always prime; m and n are always composite. We use $b_1, b_2, \ldots, b_{\phi(m)}$ as a complete list of numbers less than m and relatively prime to it.

Lemma 1 is related to our criterion for when we can simplify a congruence by dividing modulo m, but it's probably best to start with this, since this is crucial to most of what follows.

Lemma 1. *Suppose $b_i b_j \equiv b_i b_k \pmod m$. Then $b_j \equiv b_k \pmod m$, and in fact $j = k$.*

Proof. By the definition of congruence, $m \mid \left(b_i b_j - b_i b_k\right)$. Factorization allows us to rewrite this as $m \mid b_i \left(b_j - b_k\right)$. By Exercise 7.1 in the text,[1] $m \mid \left(b_j - b_k\right)$. By definition of congruence, $b_j \equiv b_k \pmod m$, which gives us the first claim.

For the second, recall our convention that $0 < b_j, b_k < m$. Perforce $-m < b_j - b_k < m$. If m divides $b_j - b_k$, the only possibility is that $b_j - b_k = 0$. The numbers are distinct, however, so $j = k$. □

Corollary 2. *Suppose $0 < a, b, c < p$ and $ab \equiv ac \pmod p$. Then $b = c$.*

Proof. $\gcd(a, p) = \gcd(b, p) = \gcd(c, p) = 1$. Apply Lemma 1. □

Corollary 3. *The list*

$$b_i b_1, b_i b_2, \ldots, b_i b_{\phi(m)}$$

is the same as the list

$$b_1, b_2, \ldots, b_{\phi(m)},$$

although the numbers may be in a different order.

Proof. We can prove this two ways. One is by using Lemma 1. The other is by noticing that if we set $a = b_i$, we can apply Lemma 10.2 in the textbook. □

What have we just shown?

- Lemma 1 shows not only that we can divide by b_i, but (importantly for our purposes) the product of $b_i b_j$ is unique to both b_i and b_j: *no other* b_k will give us $b_i b_j \equiv b_i b_k$.
- Corollary 3 shows that when we multiply any b_i by all the other b_j, we get *all* the b_k.

How does this help with these exercises? Look at the product

$$b_1 b_2 \cdots b_{\phi(m)}.$$

It is always the case that $b_1 = 1$ and $b_{\phi(m)} = m - 1 \equiv -1$, so substitution allows us to focus on

$$-b_2 b_3 \cdots b_{\phi(m)-1}.$$

Corollary 3 tells us that we can find some i such that $b_2 b_i \equiv 1$.

[1] We can prove Exercise 7.1 two ways (relying on either Bezout's Identity or the Fundamental Theorem of Arithmetic) so this is fine.

- If $i \neq 2$, then we can cancel b_2 and b_i from the product without changing the result.
- If $i = 2$, then look instead for b_j such that $b_2 b_j \equiv -1$. By Lemma 1, $j \neq 2$. So we can cancel both b_2 and b_j from the product as long as we change the sign ($\pm$) of the result.

Repeat this process with b_3, b_4, etc, and the product *must* simplify to ± 1.

We have glossed over one not-so-minor detail: is it possible that canceling b_2 and b_j causes problems for another b_k, which needs to cancel with b_2? Amazingly, the answer is no!

Lemma 4. *If* $b_i^2 \equiv 1 \pmod m$ *and* $b_i b_j \equiv -1 \pmod m$, *then* $b_j^2 \equiv 1 \pmod m$. *In particular, we can have no* b_k *such that* $b_j b_k \equiv 1$.

Proof. Assume that $b_i^2 \equiv 1$ and $b_i b_j \equiv -1$. Square both sides of the second to see that $\left(b_i b_j\right)^2 \equiv 1$. By the commutative property, $b_i^2 b_j^2 \equiv 1$. By hypothesis, $b_i^2 \equiv 1$, so substitution gives $b_j^2 \equiv 1$. Lemma 1 implies that we cannot find b_k such that $b_j b_k \equiv 1 \equiv b_j^2$. □